

Wireless (in)security @ SMAU
Fabio Pietrosanti aka Naif, ITBH

Ethical Hacker's Speech II
Smau 2002, Milano

Copyright

Questo insieme di trasparenze è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali.

Il titolo ed i copyright relative alle trasparenze (ivi inclusi, ma non limitatamente a, ogni immagine, fotografia, animazione, video e testo) sono di proprietà degli autori indicati.

Le trasparenze possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione per scopi istituzionali, non a fine di lucro.

Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente a, le riproduzioni a mezzo stampa, su supporti magnetici o su reti di calcolatori) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte dell'autore.

L'informazione contenuta in queste trasparenze è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, ecc.

L'informazione contenuta in queste trasparenze è soggetta a cambiamenti senza preavviso. Gli autori non si assumono alcuna responsabilità per il contenuto di queste trasparenze (ivi incluse, ma non limitatamente a, la correttezza, completezza, applicabilità ed aggiornamento dell'informazione).

In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste trasparenze.

In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.

Wireless, un fenomeno di moda

- Da un paio d'anni a questa parte le reti wireless sono diventate di gran moda nel campo dell'information technology
- Sembra che wireless sia la soluzione a tutti i problemi di cablaggio (LAN in centri storici, problemi di "last mile")

Wireless, è il caso? I

- Nonostante l'entusiasmo del mercato (sia dei vendor sia degli utilizzatori), dovremmo usare un minimo di "grano salis", prima di calvacare l'onda della moda
- Questo non è ciò che è accaduto e difatti le città si sono popolate di access point a standard 802.11b

Wireless, è il caso? II

- La situazione non solo è destinata a crescere esponenzialmente nel settore delle LAN ma anche in quello delle WAN

Wardriving I

- E' stato ampiamente dimostrato, anche se non pubblicizzato, il fatto che le connessioni wireless sono altamente insicure, nonostante i tentativi (del tutto infruttuosi) di rendere il protocollo quantomeno affidabile (WEP, 802.1x, estensioni proprietarie?)

Wardriving II

- E' quindi diventato fenomeno di costume anche viaggiare o passeggiare con un PDA o con un notebook (dotato di scheda wireless) per la città per controllare la presenza di reti wireless attive e il loro "grado di sicurezza"

Wardriving III




- Questo fenomeno non richiede elevate conoscenze tecniche. Sono disponibili molti tool open source con una gui abbastanza amichevole da permetterne l'uso anche ad un non addetto ai lavori

Wardriving IV

- Airsnort
- Kismet
- Wavemon
- Airtraf

Wardriving V

- Le reti sono anche segnalate, con appositi ideogrammi, per permettere a chiunque sia in grado di interpretarli di utilizzare le risorse della rete ivi presente.

let's warchalk..!	
KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid access contact  bandwidth
blackbeltjones.com/warchalking	

Wardriving VI

- Fare wardriving significa violare la legge:
 - Art 617-quater c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
 - Art 617-quinquies c.p. - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche
 - Art 615-ter c.p. - Accesso abusivo a un sistema informatico o telematico

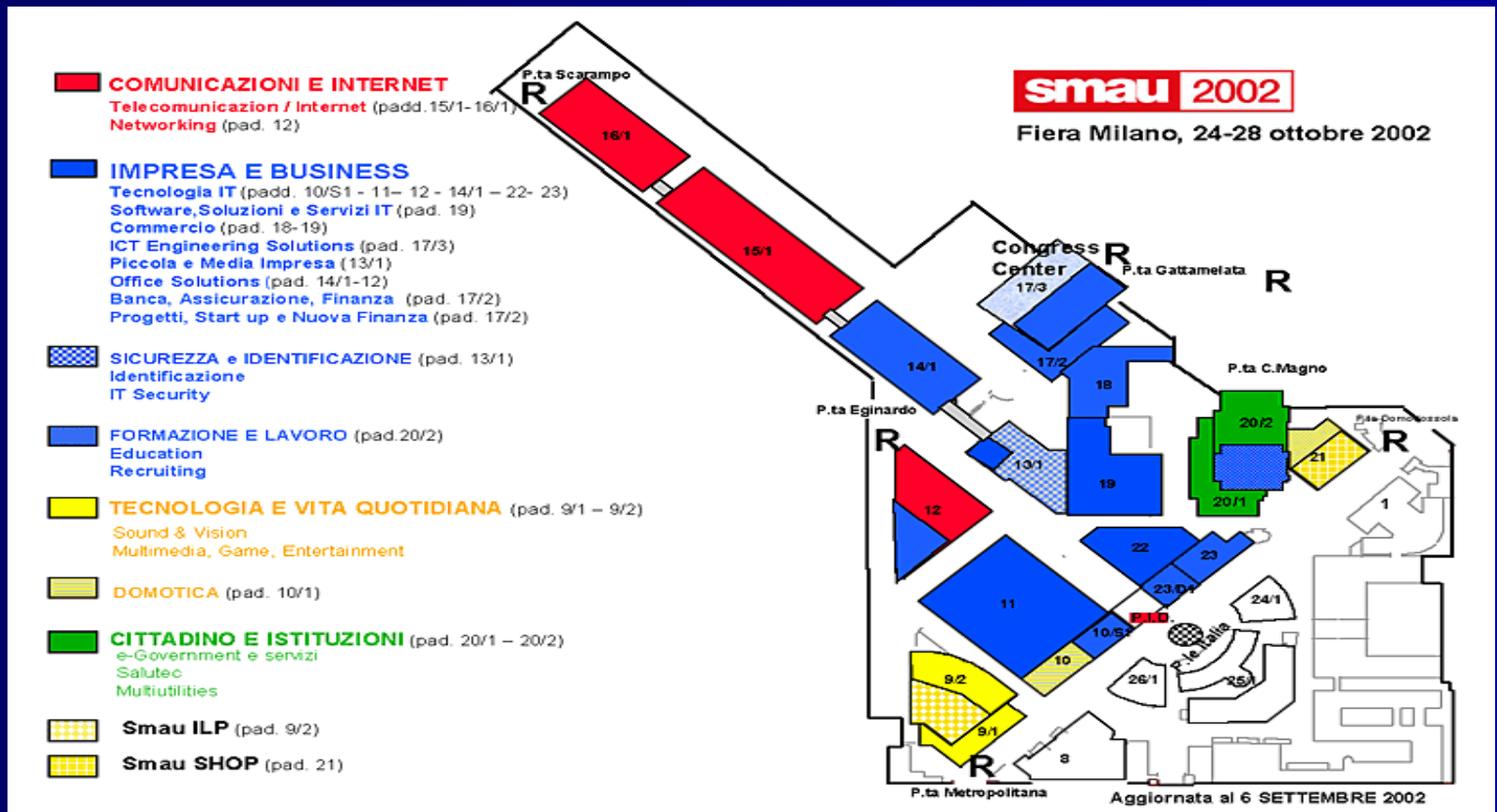
Conferme alle tendenze

- SMAU è una vetrina di prim'ordine su quelle che saranno le tendenze dell'information technology nel corso dei prossimi mesi.
- Questo è valido anche per il fenomeno "Wi-Fi" e sulla sua implementazione all'interno delle LAN aziendali

L'indagine Blackhats.it I: Intro

- Blackhats.it ha quindi provato ad effettuare, una sessione di warwalking all'interno di SMAU 2002 per farsi un'idea:
 - Del numero di reti wireless presenti nei padiglioni
 - Di quanto è stato fatto per mettere in sicurezza tali "cloud"

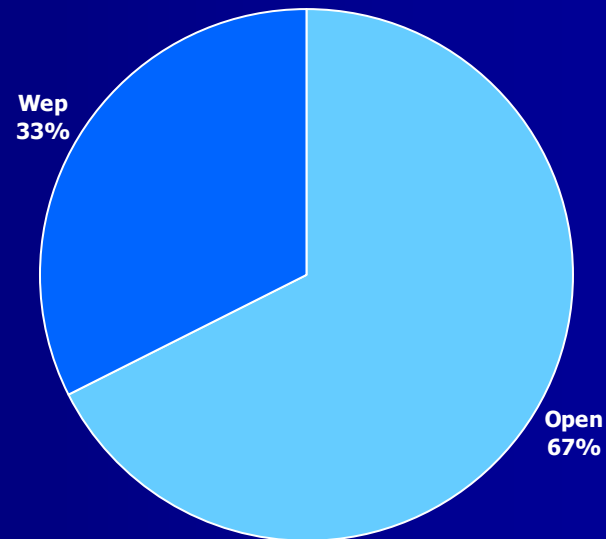
L'indagine Blackhats.it II: Mappa



L'indagine Blackhats.it

III: Risultati

- Tempo: 15 minuti
- Reti trovate: 80
- Reti protette: 28
- Reti sproteette: 58



L'indagine Blackhats.it

IV: Attrezzatura

- Computer Portatile
- Scheda Wireless (prism2 ?)
- Antenna ad alto guadagno
- Auricolare

L'indagine Blackhats.it V: E la legge?

E' una ricerca

Non essendoci l'intenzione fraudolenta nell'analizzare (intercettare) i dati passanti sui 2.4ghz e non andando mai in nessun modo a controllare il contenuto dei pacchetti in transito ma solo alcuni specifici campi dell'intestazione (header) di questi ultimi, siamo al riparo dall'infrangere leggi sulle intercettazioni;

Inoltre non essendoci mai associati agli Access Point rilevati, non ci siamo mai abusivamente introdotti in un sistema informatico mettendoci al riparo dal violare l'Art 615-ter c.p.

Conclusioni

- La sicurezza dei protocolli nasce da un buon design
- Lo standard 802.11 e' insicuro?
 - Chi e' il vostro attacker?
 - Cosa dovete proteggere?
- La ricerca e' l'unica via

Wireless (in)security @ SMAU 02

Fabio Pietrosanti (naif)

Ethical Hacker's Speech II

Smau, 26 Ottobre 2002

Contacts:

info@blackhats.it

<http://www.blackhats.it>